Eric H. Gibbs (State Bar No. 178658)
ehg@girardgibbs.com
Matthew B. George (State Bar No. 239322)
mbg@girardgibbs.com
Jennifer L. McIntosh (State Bar No. 264903)
jlm@girardgibbs.com
GIRARD GIBBS LLP
601 California Street, 14th Floor
San Francisco, California 94104
Telephone: (415) 981-4800
Facsimile: (415) 981-4846

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

SHONNA EARLS and JOHN HOLT SR., on behalf of themselves and all others similarly situated,

Plaintiffs,

vs.

THE HOME DEPOT, INC. and HOME DEPOT U.S.A., INC.,

Defendants.

Case No. 3:14-cv-4315

CLASS ACTION

COMPLAINT FOR RELIEF BASED ON:

(1) Violation of the California Customer Records Act;
(2) Violation of the California Unfair Competition Law; and
(3) Negligence

DEMAND FOR JURY TRIAL

SUMMARY OF THE CASE

1. Starting in April 2014 and continuing for several months, the debit and credit card information of millions of Home Depot customers was stolen from Home Depot's in-store credit and debit card processing system. Because of the data breach, customers' debit and credit card information quickly flooded the black market, resulting in fraudulent charges, an increased risk of identity theft, and other harms to unsuspecting consumers.

2. On September 2, 2014, news media outlets began reporting on a potential data breach affecting Home Depot customers in the United States. Home Depot confirmed the data breach a week later and began notifying its customers that their credit card and debit card information may have been compromised. On September 18, 2014, Home Depot confirmed that 56 million credit and debit cards were exposed in the data breach. Despite the ever increasing number of nationwide retailers being targeted for similar data breaches, Home Depot allowed its customers to be exposed by failing to exercise reasonable security precautions and failing to comply with industry standards for processing debit and credit card information. Had Home Depot taken necessary precautions to protect its customers, it would have prevented the breach altogether or detected it much sooner, reducing the harm its customers are now suffering.

3. Plaintiffs Shonna Earls and John Holt Sr. are Home Depot customers who bring this proposed class action lawsuit on behalf of Home Depot customers nationwide alleging that Home Depot failed to adequately safeguard its customers' credit and debit card information in compliance with applicable statutes. Plaintiffs seek injunctive relief requiring Home Depot to invest in security to comply with regulations designed to prevent these types of breaches, damages, restitution, and other remedies.

PARTIES

4. Plaintiff Shonna Earls is a resident of Contra Costa County, California.

5. Plaintiff John Holt Sr. is a resident of Madera County, California.

6. Defendant The Home Depot, Inc. is incorporated in the State of Delaware, with its principal place of business in Atlanta, Georgia.

7. Defendant Home Depot U.S.A., Inc. is a domestic subsidiary of The Home Depot, Inc. (collectively, "Home Depot"). Similarly, it is incorporated in the State of Delaware, with its principal place of business in Atlanta, Georgia. Home Depot is one of the top five largest retailers by revenue in the United States with nearly 2,000 stores in the United States.

JURISDICTION AND VENUE

8. This Court has original jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because (a) at least one member of the putative class is a citizen of a state different from Defendant, (b) the amount in controversy exceeds $5,000,000, exclusive of interest and costs, (c) the proposed class consists of more than 100 class members, and (d) none of the exceptions under the subsection apply to this action.

9. This Court has jurisdiction over Home Depot because Home Depot U.S.A., Inc. is registered to conduct business in California, Home Depot has sufficient minimum contacts in California, or otherwise intentionally avails itself of the markets within California, through the promotion, sale, marketing and distribution of its products in California, to render the exercise of jurisdiction by this Court proper and necessary.

10. Venue is proper in this District under 28 U.S.C. § 1391 because Plaintiff Earls resides in this district and a substantial part of the events giving rise to Plaintiff Earls' claims occurred in this District.

INTRADISTRICT ASSIGNMENT

11. Assignment is proper to the San Francisco division of this District under Local Rule 3-2(c), as a substantial part of the events and omissions giving rise to Plaintiff Earls' claims occurred in Contra Costa County.

COMMON FACTUAL ALLEGATIONS

12. When a customer makes a purchase at Home Depot, the stores' payment card systems take "track data" stored on the magnetic strip of the card swiped. Track data can include customers' names, card numbers, card expiration dates, and CVV codes (security codes that are stored in the magnetic strip of the card). Once someone has track data from a credit card or debit card, they can create new cards and make fraudulent purchases at stores or over the internet. This type of consumer

data is incredibly valuable on the black market, and is the type of consumer data hackers have been routinely stealing from retailers, including in a number of highly publicized breaches against Target, Michael's, and Neiman Marcus.

13. On September 2, 2013, information security reporter Brian Krebs announced that he had learned from confidential sources that Home Depot was the latest retailer hit by a data breach. Mr. Krebs also reported that massive batches of stolen credit cards and debit cards traced back to customers who shopped at Home Depot were being sold on the online black market. According to reports, Home Depot began investigating the data breach on the same day.

14. On September 8, 2014, Home Depot issued a press release confirming that its payment systems had been breached, and that it "could potentially impact customers using payment cards at its U.S. and Canadian stores," from April 2014 and on. Ten days later, Home Depot confirmed that 56 million customers' credit and debit cards were exposed in the data breach, leading some media outlets to label it as the largest retail data breach that may result in fraudulent charges of up to $3 billion. Some experts have also commented that the Home Depot data breach may be one of the largest data breaches to ever strike a retailer, even larger than the Target data breach that affected approximately 40 to 70 million people.

15. Despite the prevalence of hackers exploiting lax security protocols at large retailers, The New York Times reported that former Home Depot employees have come forward anonymously to indicate that Home Depot "was slow to respond to early threats and only belatedly took action," and that "[Home Depot] relied on outdated software to protect its network and scanned systems that handled customer information irregularly."[1]

16. The Home Depot data breach is not the first of its kind. Data breaches aimed at major corporations have risen dramatically in recent years. A number of corporations have experienced widely-publicized data breaches, including TJX Companies Inc. in 2007, Heartland Payment Systems in January 2009, Schnuck Markets Inc. in April 2013, Target in December 2013, Neiman Marcus in January 2014, and Michaels Stores in April 2014. Given the recent increase of data breaches aimed at

[1] Julie Creswell & Nicole Perlroth, *Ex-Employees Say Home Depot Left Data Vulnerable*, The New York Times (Sept. 19, 2014) http://www.nytimes.com/2014/09/20/business/ex-employees-say-home-depot-left-data-vulnerable.html.

major retailers, businesses such as Home Depot should be more vigilant than ever of the need to adopt, implement, and maintain security measures to protect customers' personal information.

Retail Data Security Standards

17. Although not exhaustive of adequate security measures that must be constantly evaluated and tested, the Payment Card Industry ("PCI") Data Security Standard provides an industry baseline for how retailers like Home Depot must secure credit and debit card data. The PCI Security Standards Council is the organization that publishes the standards and was created by the major credit card issuer companies to create uniform security standards. Major credit card companies like Visa and MasterCard require that merchants that accept their credit and debit cards comply with PCI standards. Using the PCI standards as a guideline, it is clear that Home Depot breached numerous PCI standards resulting in the data breach of this size and scope.

18. PCI standards are built around a core set of security goals and have detailed instructions for compliance within each requirement. The 12 requirements and goals PCI compliance are:

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Complying with these standards is critical to protecting customer debit and credit information.

19. The fact that thieves were able to take the debit and credit card information of millions of people who shopped at Home Depot over a period of several months shows that one of Home Depot's major failures was not properly monitoring their security systems for breaches or non-permitted access

to areas where sensitive should be segregated and securely stored. PCI standards require companies to monitor all system components at least daily. PCI Standards, Version 3.0, Requirement 10.6, p. 87.

20. Home Depot also failed to properly encrypt its customers' data in violation of the PCI and industry standards. Strong encryption measures are necessary so that if data is improperly accessed it would be unusable and indecipherable to criminals who want to use it for illegal purposes. The rapid availability of Home Depot's customers' *unencrypted* data on the black market means Home Depot was either not encrypting the data at all, or using lax encryption standards that allowed thieves to quickly and easily decrypt it.

21. The PCI Council has stated that it is ultimately the retailer's responsibility to make sure that it is in compliance with PCI standards. Bob Russo, the general manager of the PCI Standard Council explains: "It's up to the merchant to make sure they stay in compliance and that they are secure. For each of those [big public] breaches credit card companies looked at the logs [and found] that none of them was compliant at the time of the breach." He also stated: "A layered approach to security is absolutely necessary to protect sensitive payment card data – without ongoing vigilance or a comprehensive security strategy, organizations may be just a change control away from noncompliance. Organizations must make protecting cardholder data a daily priority, not a one-time exercise." Mr. Russo has also said that when merchants have their PCI compliance audited, it just shows "a snapshot in time." He went on to say, "You could be compliant and five minutes later you don't apply a patch and you aren't compliant anymore."

22. Furthermore, it is commonly recognized in the security industry that PCI compliance is only the starting point for taking reasonable security measures to protect credit and debit card data. Mr. Russo stated, "It's important to remember that the PCI [standard] is the floor for card data security, not the ceiling." Michael Maloof, Chief Technology Officer of TriGeo Network Security stated, "Any business foolish enough to simply make compliance their only security goal has made a serious, and sometimes fatal, mistake." He also stated, "Companies have embraced the intent of the regulations and have accepted the responsibility to secure their networks, train their employees and maintain a state of vigilance to ensure their systems remain secure. Other companies see PCI as yet another tax on their businesses and do everything they can to pay as little as possible-that is, until they are forced to pay for

the consequences." Given that the data from millions of accounts over several months was stolen, it is clear that Home Depot failed to maintain a state of vigilance over its security system and did not comply with PCI standards.

23. As a result of data breaches of this size and scope, and much like victims of other data breaches, Home Depot customers have and will have to spend time and money securing their accounts and protecting their identities. Home Depot customers who have unauthorized purchases may have to pay fees to their banks to pay for new debit or credit cards, or have to pay fees to have the cards shipped faster so that they do not have to wait weeks to make purchases on their accounts. Home Depot customers may also incur bank fees associated with fraudulent over-drafting of their accounts and late fees from third-parties that use automated billing because consumers will have to close accounts used for those payments or may have insufficient funds to pay them. As Home Depot itself recommended, customers will need to monitor their accounts and credit, and will also have to pay for credit monitoring or credit reports in the wake of the data breach to make sure that their credit is not harmed by anyone who may have stolen their information.

24. Many people who were affected by the data breach will also have lost access to their funds on the debit and credit cards compromised, and will have to wait for their banks to send them new cards while meeting regular financial obligations. Likewise, some Home Depot customers will lose time and money by spending hours on the phone or in person with banks and credit agencies trying to reverse unauthorized charges, clear up credit issues, and order new cards.

PLAINTIFFS' EXPERIENCE

Plaintiff Shonna Earls

25. Ms. Earls is a resident of Contra Costa, California. On August 18, 2014, she used her San Francisco Federal Credit Union Visa credit card to make a purchase at a Home Depot store in El Cerrito, California. In early September 2014, she incurred seven unauthorized charges totaling to $543.95 on the same credit card she had used at Home Depot. After promptly notifying her bank of these unauthorized charges and spending time to resolve the issue, her bank reversed her charges in the form of a provisional credit. The data breach has caused harm to Plaintiff Earls because her personal and financial information associated with her card has been compromised as a result of the data breach.

Plaintiff Earls is also at risk for future identity fraud due to her information being stolen from Home Depot and sold on the online black market.

Plaintiff John Holt Sr.

26. Mr. Holt Sr., a resident of Madera County, California, has a debit card with Merco Credit Union, which he used to make a purchase at a Home Depot store in Madera, California on July 6, 2014. On September 5, 2014, his bank notified him that an unauthorized address verification was attempted on his debit card and that a replacement debit card would be sent to him. Plaintiff Holt's personal information associated with his debit card was compromised in and as a result of the Home Depot data breach. Plaintiff Holt has been harmed by having his financial and personal information compromised and is at risk for future identity fraud due to his information being stolen from Home Depot and sold on the online black market.

CLASS ACTION ALLEGATIONS

27. Plaintiff Shonna Earls and Plaintiff John Holt Sr. bring this action pursuant to Federal Rule of Civil Procedure 23 on behalf of themselves and the classes preliminarily defined as:

Nationwide Class

> All Home Depot customers in the United States whose personal information was compromised as a result of the data breach announced by Home Depot in September 2014.

California Class

> All Home Depot customers residing in California who made purchases with a debit or credit card at a Home Depot store within three years of the filing of this lawsuit through the present.

Excluded from the proposed classes are Home Depot; any agent, affiliate, parent, or subsidiary of Home Depot; any entity in which Home Depot has a controlling interest; any officer or director of Home Depot; any successor or assign of Home Depot; anyone employed by counsel for Plaintiffs in this action; and any Judge to whom this case is assigned, as well as his or her staff and immediate family.

28. Plaintiffs satisfy the numerosity, commonality, typicality, and adequacy prerequisites for suing as a representative party pursuant to Rule 23.

29. Numerosity. The proposed classes consist of millions of Home Depot customers who had their data stolen in the Home Depot data breach, making joinder of each individual member impracticable.

30. Commonality. Common questions of law and fact exist for each of the proposed class's claims and predominate over questions affecting only individual class members.

For the Nationwide Class, common questions include:

a. Whether Home Depot had a legal duty to use reasonable security measures to protect class members' credit and debit card information;

b. Whether Home Depot breached its legal duty by failing to protect class members' credit and debit card information;

c. Whether Home Depot acted reasonably in securing its customer data;

d. Whether any breach of Home Depot's legal duties caused Plaintiffs and the class members to suffer damages; and

e. Whether Plaintiffs and class members are entitled to damages, restitution and injunctive relief.

For the California Class, common questions include:

a. Whether Home Depot violated California Civil Code sections 1798.81 and 1798.81.5 by failing to implement reasonable security procedures and practices;

b. Whether Home Depot violated California Civil Code section 1798.82 by failing to promptly notify class members that their personal information had been compromised;

c. Whether class members may obtain injunctive relief against Home Depot under Civil Code section 1798.84 or under the UCL; and

d. What security procedures and data-breach notification procedure should Home Depot be required to implement as part of any injunctive relief ordered by the Court.

31. Typicality. Plaintiffs' claims are typical of the claims of the proposed classes because, among other things, Plaintiffs and class members sustained similar injuries as a result of Home Depot's uniform wrongful conduct and their legal claims all arise from the same core Home Depot practice.

32. Adequacy. Plaintiffs will fairly and adequately protect the interests of the classes. Their interests do not conflict with class members' interests and they have retained counsel experienced in complex class action litigation and data privacy to vigorously prosecute this action on behalf of the classes.

33. In addition to satisfying the prerequisites of Rule 23(a), Plaintiffs satisfy the requirements for maintaining a class action under Rule 23(b)(3). Common questions of law and fact predominate over any questions affecting only individual members and a class action is superior to individual litigation. The amount of damages available to individual plaintiffs is insufficient to make litigation addressing Home Depot's conduct economically feasible in the absence of the class action procedure. Individualized litigation also presents a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system presented by the legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

34. In addition, class certification is appropriate under Rule 23(b)(1) or (b)(2) because:

a. the prosecution of separate actions by the individual members of the proposed classes would create a risk of inconsistent or varying adjudication which would establish incompatible standards of conduct for Home Depot;

b. the prosecution of separate actions by individual class members would create a risk of adjudications with respect to them which would, as a practical matter, be dispositive of the interests of other class members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; and

c. Home Depot has acted or refused to act on grounds that apply generally to the proposed classes, thereby making final injunctive relief or declaratory relief described herein appropriate with respect to the proposed classes as a whole.

/ / /

FIRST CAUSE OF ACTION

For Violation of the California Customer Records Act, California Civil Code Section 1798.80, *et seq.*

35. Plaintiffs incorporate the above allegations by reference.

36. Plaintiffs bring this cause of action on behalf of all current Home Depot customers residing in California who made purchases with a debit or credit card at a Home Depot store within three years of the filing of this lawsuit through the present.

37. "[T]o ensure that personal information about California residents is protected," the California Legislature enacted Civil Code section 1798.81.5, which requires that any business that "owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

38. Home Depot is a "business" within the meaning of Civil Code section 1798.80(a).

39. Plaintiffs and members of the Class are "customer[s]" within the meaning of the Civil Code section 1798.80(c) "who provide[d] personal information to [Home Depot] for the purpose of purchasing or leasing a product or obtaining a service from the business." Pursuant to Civil Code sections 1798.80(e) and 1798.81.5(d)(1)(C), "personal information" includes debit card and credit card information.

40. The breach of the data of the debit and credit card information of millions of accounts of Home Depot customers constituted a "breach of the security system" of Home Depot pursuant to Civil Code section 1798.82(g).

41. By keeping customers' personal data within its custody and control longer than necessary, and by failing to properly and adequately dispose or make customers' data undecipherable, Home Depot violated section 1798.81.

42. By failing to implement reasonable measures to protect its customers' personal data, Home Depot violated Civil Code section 1798.81.5.

43. In addition, by failing to promptly notify all affected Home Depot customers that their personal information had been acquired (or was reasonably believed to have been acquired) by

unauthorized persons in the data breach, Home Depot violated Civil Code section 1798.82 of the same title.

44. By violating Civil Code sections 1798.81, 1798.81.5 and 1798.82, Home Depot "may be enjoined" under Civil Code section 1798.84(e).

45. Accordingly, Plaintiffs request that the Court enter an injunction requiring Home Depot to implement and maintain reasonable security procedures to protect customers' data in compliance with the California Customer Records Act, including, but not limited to: (1) ordering that Home Depot, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Home Depot's systems on a periodic basis; (2) ordering that Home Depot engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (3) ordering that Home Depot audit, test, and train its security personnel regarding any new or modified procedures; (4) ordering that Home Depot, consistent with industry standard practices, segment customer data by, among other things, creating firewalls and access controls so that if one area of Home Depot is compromised, hackers cannot gain access to other portions of Home Depot's systems; (5) ordering that Home Depot purge, delete, destroy in a reasonable secure manner customer data not necessary for its provisions of services; (6) ordering that Home Depot, consistent with industry standard practices, conduct regular database scanning and securing checks; (7) ordering that Home Depot, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (8) ordering Home Depot to meaningfully educate its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Home Depot customers must take to protect themselves.

46. Plaintiffs further request that the Court require Home Depot to (1) identify and notify all members of the Class who have not yet been informed of the data breach; and (2) to notify affected customers of any future data breaches by email within 24 hours of Home Depot's discovery of a breach or possible breach and by mail within 72 hours.

47. As a result of Home Depot's violation of Civil Code sections 1798.81, 1798.81.5, and 1798.82, Plaintiffs and members of the Class have and will incur economic damages relating to time and money spent remedying the breach, expenses for bank fees associated with the breach, late fees from automated billing services associated with the breach, lack of access to funds while banks issue new cards, as well as the costs of credit monitoring and purchasing credit reports.

48. Plaintiffs, individually and on behalf of the members of the Class, seek all remedies available under Civil Code section 1798.84, including, but not limited to: (a) damages suffered by members of the Class; and (b) equitable relief.

49. Plaintiffs, individually and on behalf of the members of the Class, also seeks reasonable attorneys' fees and costs under applicable law.

SECOND CAUSE OF ACTION

For Unlawful and Unfair Business Practices Under California Business and Professions Code § 17200, *et seq.*

50. Plaintiffs incorporate the above allegations by reference.

51. Plaintiffs bring this cause of action on behalf of all Home Depot customers whose personal information was compromised as a result of the data breach announced by Home Depot in September 2014.

52. Home Depot's acts and practices, as alleged in this complaint, constitute unlawful and unfair business practices, in violation of the Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17200, *et seq*.

53. Home Depot's acts and practices, as alleged in this complaint, constitute unlawful practices in that they violate the California Customer Records Act, Civil Code section 1798.80, *et seq*.

54. Home Depot's practices were unlawful and in violation of Civil Code sections 1798.81 and 1798.81.5(b) of the California Customer Records Act because Home Depot failed to take reasonable security measures in protecting its customers' data.

55. Home Depot's practices were also unlawful and in violation of Civil Code section 1798.82 because Home Depot unreasonably delayed informing Plaintiffs and members of the Class about the breach of security after Home Depot knew the data breach occurred.

56. The acts, omissions, and conduct of Home Depot constitutes a violation of the unlawful prong of the UCL because they failed to comport with a reasonable standard of care and California public policy as reflected in statutes such as the Online Privacy Protection Act, Cal. Bus. & Prof. Code § 22576, and the Information Practices Act of 1977, Cal. Civ. Code § 1798, *et seq.*, which seek to protect customer data and ensure that entities who solicit or are entrusted with personal data utilize reasonable security measures.

57. By failing to take reasonable security measures to protect its customers' data, Home Depot engaged in unfair business practices and conduct that undermines or violates the stated policies underlying the California Customer Records Act. Home Depot's failure to take reasonable security measures to protect its customers' data violates the stated policy of the Legislature in that businesses are to protect the personal information of their customers.

58. In unduly delaying informing customers of the data breach, Home Depot engaged in unfair business practices by engaging in conduct that undermines or violates the stated policies underlying the California Customer Records Act and other privacy statutes. In enacting the California Customer Records Act, the Legislature stated that: "[i]dentity theft is costly to the marketplace and to consumers" and that "victims of identity theft must act quickly to minimize the damage; therefore expeditious notification of possible misuse of a person's personal information is imperative." 2002 Cal. Legis. Serv. Ch. 1054 (A.B. 700) (WEST). Home Depot's conduct also undermines California public policy as reflected in other statutes such as the Online Privacy Protection Act, Cal. Bus. & Prof. Code § 22576, and the Information Practices Act of 1977, Cal. Civ. Code § 1798, *et seq.*, which seek to protect customer data and ensure that entities who solicit or are entrusted with personal data utilize reasonable security measures.

59. As a direct and proximate result of Home Depot's unlawful and unfair business practices as alleged herein, Plaintiffs and members of the Class have suffered injury in fact. Plaintiffs and the Class have been injured in that their personal and financial information has been compromised and are at risk for future identity theft and fraudulent activity on their financial accounts, which is evidenced by reports that some of the stolen credit and debit card information are being sold on the online black market.

60. While failing to implement reasonable security measures to protect its customers' personal data, Home Depot continued to unjustly enrich itself by reaping profits from its business transactions with its customers and gaining an unfair market advantage.

61. As a result of Home Depot's violations, Plaintiffs and members of the Class are entitled to injunctive relief, including, but not limited to: (1) ordering that Home Depot, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Home Depot's systems on a periodic basis; (2) ordering that Home Depot engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (3) ordering that Home Depot audit, test, and train its security personnel regarding any new or modified procedures; (4) ordering that Home Depot, consistent with industry standard practices, segment customer data by, among other things, creating firewalls and access controls so that if one area of Home Depot is compromised, hackers cannot gain access to other portions of Home Depot's systems; (5) ordering that Home Depot purge, delete, destroy in a reasonable secure manner customer data not necessary for its provisions of services; (6) ordering that Home Depot, consistent with industry standard practices, conduct regular database scanning and securing checks; (7) ordering that Home Depot, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (8) ordering Home Depot to meaningfully educate its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Home Depot customers must take to protect themselves.

62. Because of Home Depot's unfair and unlawful business practices, Plaintiffs and the Class are entitled to relief, including restitution to Plaintiffs and Class members of their costs incurred associated with the data breach and disgorgement of all profits accruing to Home Depot because of its unlawful and unfair business practices, attorneys' fees and costs, declaratory relief, and a permanent injunction enjoining Home Depot from its unlawful and unfair practices.

THIRD CAUSE OF ACTION

Negligence

63. Plaintiffs incorporate the above allegations by reference.

64. Plaintiffs bring this cause of action on behalf of all Home Depot customers in the United States whose personal information was compromised as a result of the data breach announced by Home Depot in September 2014.

65. In collecting the debit and credit card information of its customers, Home Depot owed Plaintiffs and members of the Class a duty to exercise reasonable care in safeguarding and protecting that information. This duty included, among other things, maintaining and testing Home Depot's security systems and taking other reasonable security measures to protect and adequately secure the personal data of Plaintiffs and the Class from unauthorized access. Home Depot's security system and procedures for handling the debit and credit card information of its customers were intended to affect Plaintiffs and the Class. Home Depot was aware that by taking the debit and credit card information of its customers, it had a responsibility to take reasonable security measures to protect the data from being stolen.

66. The duty Home Depot owed to Plaintiffs and members of the Class to protect their personal information is also underscored by the California Customer Records Act, which was created specifically to protect customers who provide personal information to businesses during transactions with those businesses.

67. Additionally, Home Depot had a duty to timely disclose to Plaintiffs and members of the Class that their debit card and credit card information had been or was reasonably believed to have been compromised. Timely disclosure was appropriate so that Plaintiffs and members of the Class could, among other things, monitor their credit card or debit card accounts, undertake appropriate measures to avoid unauthorized charges on their debit card or credit card accounts, and change or cancel their debit or credit card PINs (personal identification numbers) to prevent or mitigate the risk of fraudulent cash withdrawals or unauthorized transactions.

68. There is a very close connection between Home Depot's failure to take reasonable security standards to protect its customers' data and the injury to Plaintiffs and the Class. When

customers have their debit and credit card information stolen, they are at risk for identity theft, and need to buy credit monitoring services and purchase credit reports to protect themselves from identity theft.

69. Home Depot is morally to blame for not protecting the data of its customers by failing to take reasonable security measures. If Home Depot had taken reasonable security measures, data thieves would not have been able to take the debit and credit card information of millions of accounts of Home Depot shoppers over a period of months.

70. The policy of preventing future harm weighs in favor of finding a special relationship between Home Depot and the Class. Customers count on Home Depot to keep their data safe. If companies are not held accountable for failing to take reasonable security measures to protect customers' debit and credit card information, they will not take the steps that are necessary to protect against future data breaches.

71. It was foreseeable that if Home Depot did not take reasonable security measures, the data of Plaintiffs and members of the Class would be stolen. Major retailers like Home Depot face a higher threat of security breaches than other smaller businesses due in part to the millions of customers they transact business with. Home Depot should have known to take precaution to secure its customers' data, especially in light of the recent data breaches affecting numerous retailers, including Target, Michaels Stores, and Neiman Marcus.

72. Home Depot breached its duty to exercise reasonable care in protecting the personal information of Plaintiffs and the Class by failing to implement and maintain adequate security measures to safeguard its customers' personal information, failing to monitor its point of sale systems to identify suspicious activity, and allowing unauthorized access to the personal information of Plaintiffs and the Class.

73. Home Depot breached its duty to timely notify Plaintiffs and the Class about the data breach by waiting several days after discovering the data breach to inform Plaintiffs and members of the Class that their debit card and credit card information had been or was reasonably believed to have been compromised.

74. But for Home Depot's failure to implement and maintain adequate security measures to protect its customers' personal information and failure to monitor its point of sale systems to identify

suspicious activity, the personal information of Plaintiffs and members of the Class would not be stolen, their identities and financial accounts would not be subject to fraud, and they would not be at a heightened risk of identity theft in the future.

75. Home Depot's negligence was a substantial factor in causing harm to Plaintiffs and members of the Class.

76. As a direct and proximate result of Home Depot's failure to exercise reasonable care and use commercially reasonable security measures, the debit and credit information of Home Depot customers was accessed by unauthorized individuals who could use, and have used, the information to commit debit and credit card fraud. Plaintiffs and the Class face a heightened risk of identity theft in the future, which is evidenced by reports that some of the stolen credit and debit card information are being sold on the online black market.

77. Plaintiffs and members of the Class have also suffered economic damages.

78. Neither Plaintiffs nor other members of the Class contributed to the security breach, nor did they contribute to Home Depot's employment of insufficient security measures to safeguard customers' debit and credit card information.

79. Plaintiffs and the Class seek compensatory damages and punitive damages with interest, the costs of suit and attorneys' fees, and other and further relief as this Court deems just and proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the proposed classes, requests that the Court:

a. Certify this case as a class action on behalf of the classes defined above, appoint Shonna Earls and John Holt Sr. as class representatives, and appoint their counsel as class counsel;

b. Award injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and other class members;

c. Award damages to Plaintiffs and class members in an amount to be determined at trial;

d. Award Plaintiffs and class members their reasonable litigation expenses and attorneys' fees;

e. Award Plaintiffs and class members pre- and post-judgment interest, to the extent allowable; and

f. Award such other and further relief as equity and justice may require.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury for all issues so triable.

Dated: September 24, 2014

Respectfully Submitted,

GIRARD GIBBS LLP

By: /s/ Eric H. Gibbs
Eric H. Gibbs

Matthew B. George
Jennifer L. McIntosh
601 California Street, 14th Floor
San Francisco, California 94108
Telephone: (415) 981-4800
Facsimile: (415) 981-4846